WEB 2.0 SUMMIT
6:NOVEMBER:08
Transforming the Network to an Enterprise for the Warfighter
LTG Jeff Sorenson
Chief Information Officer/G-6
AMERICA'S ARMY: THE STRENGTH OF THE NATION
ARMY STRONG

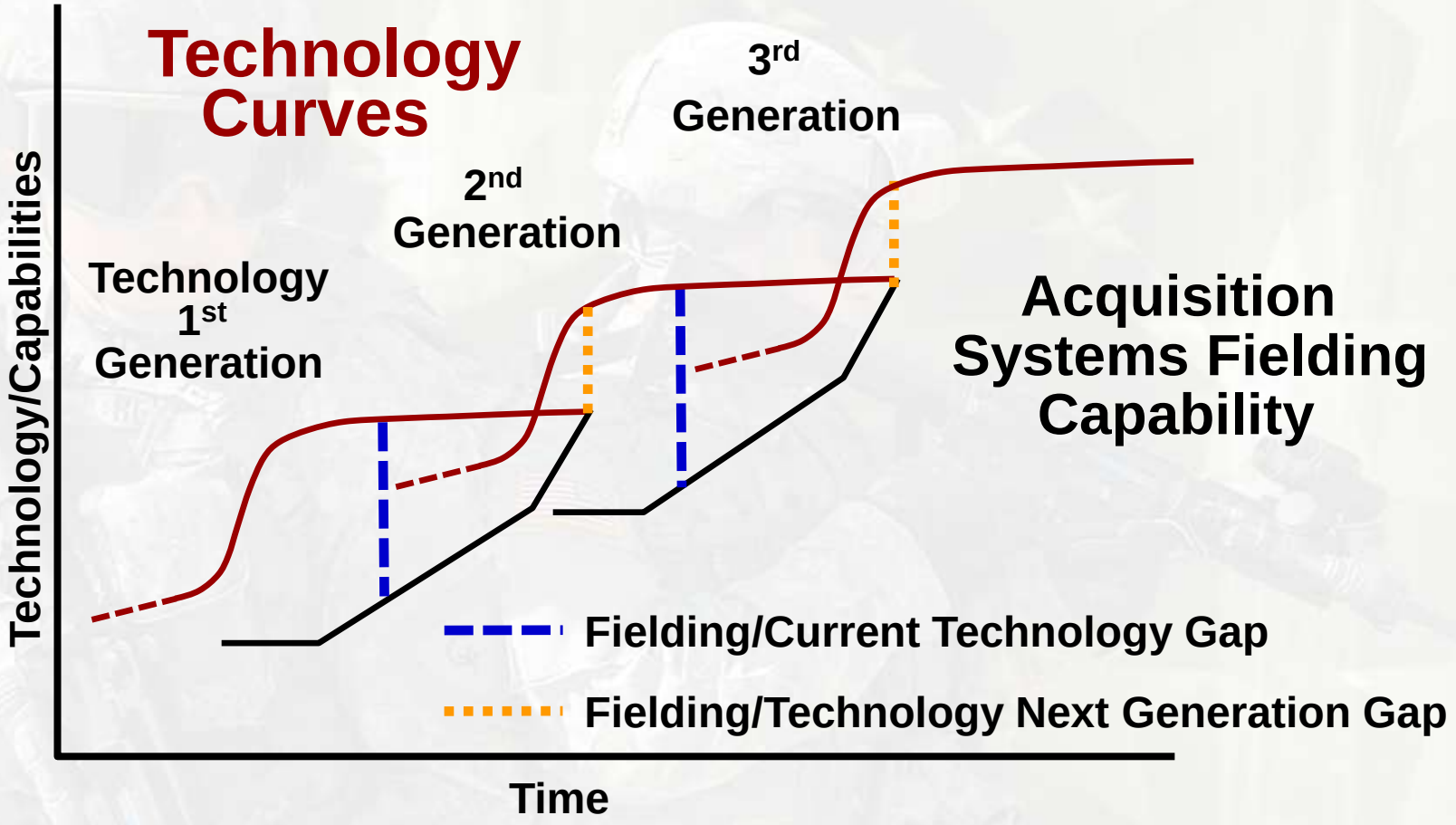
Agenda

- Era of Persistent Conflict
- Information Technology Cycles
  - IT Requirements & Methodology
  - Looking Back – What It Means
- Web 2.0 & Networking for the Warfighter
  - Warfighter Forums
  - Battle Command
  - Cyber Warfare
- Conclusions

Era of Persistent Conflict

Protracted confrontation . . . fueled by *six important trends*

Current Acquisition/Fielding



Results – Capability to the Field Significantly Lags Behind Technology

king Back – What It Means

All in less than one lifetime!

TACTICA
INTERNE
DIGITIZATIO
& WEB-SVC
???

MSE development 1980

ASAS Block I 1984

SINCGARS production 1987

GPS used Desert Storm 1991

Digitization initiated 1994

Tactical Internet 1997

Digitization 1999+

2003

2004

Desert One 1980

Urgent Fury 1983

Just Cause 1989-90

Desert Storm 1991

Uphold Democracy 1994-95

Joint Endeavor 1995+

Enduring Freedom 2001+

Iraqi Freedom 2003+

Katrina 2005

1965 Moore's Law

1969 ARPANET is born

1980 Internet protocols

1983 •TCP/IP – ARPANET

1984 CISCO

1985 Windows 1.0

1989 Internet 100,000 hosts

1990 "World Wide Web"

1992 Internet 1,000,000 hosts

1994 Shopping malls on net;

1995 Sun – JAVA; Operation Home Front

1997 "weblog" coined;

2002 Internet 171,000,000 hosts

2004 Google goes public; ~85% all searches

12/07 > 112 million blogs

2005 Internet 350,000,000 hosts; 8,000,000 blogs

INTERNET

WEB 1.0

WEB 2.0

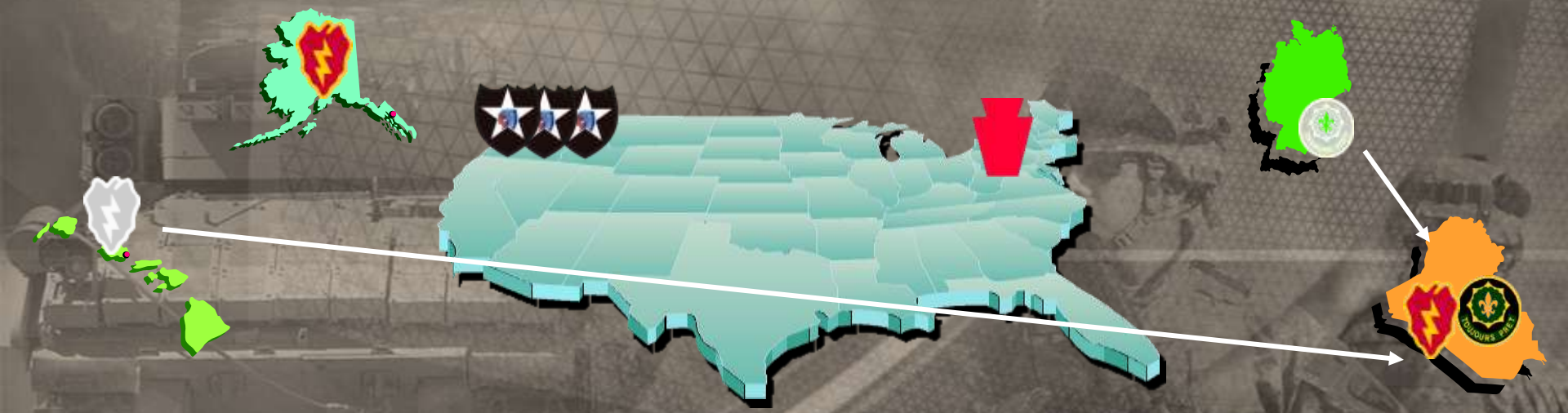
Stryker Light Armored Vehicle-III

Stryker LAV-III

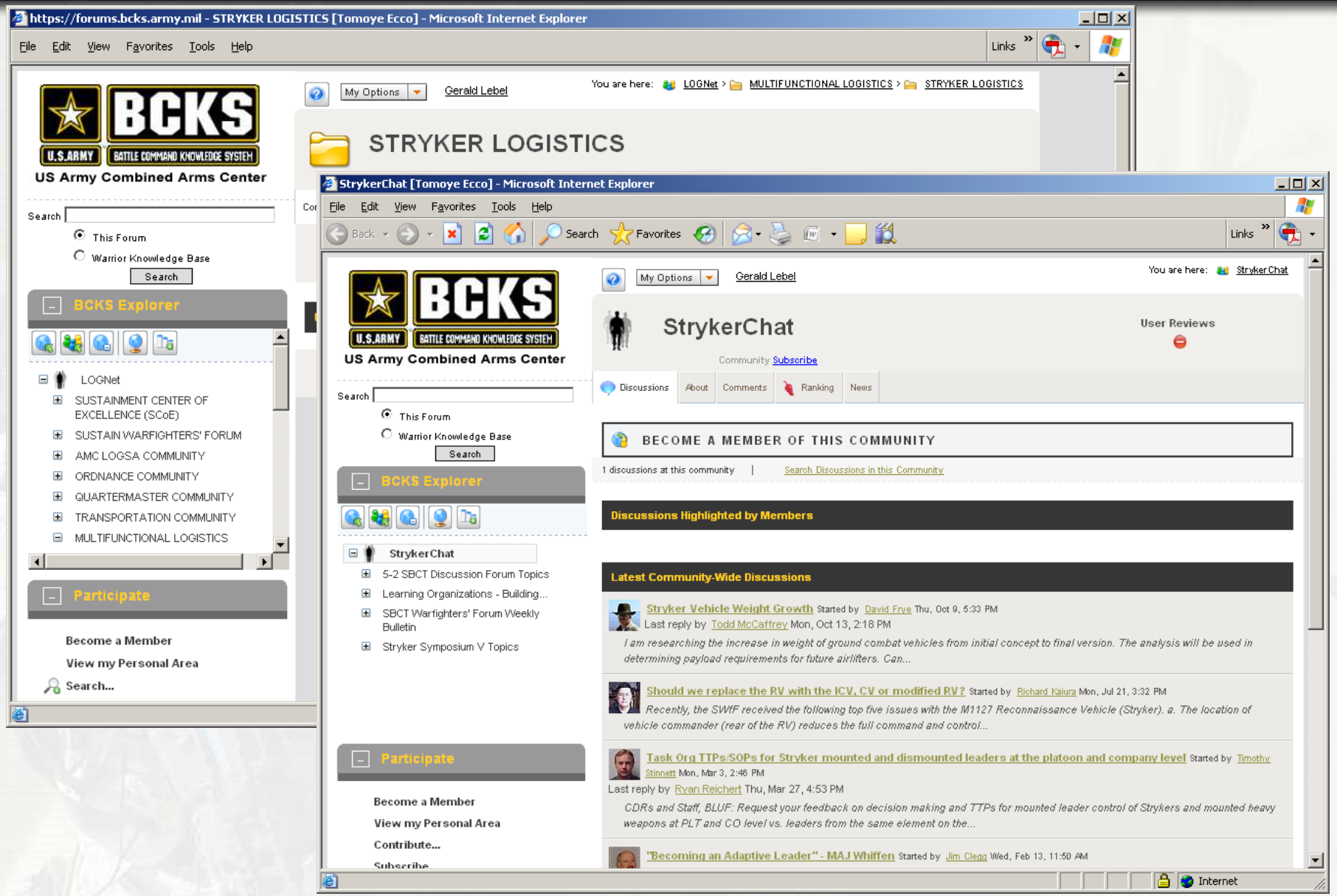
- Family of Vehicles (Nov 2000)
  - 2 main Variants: Infantry Carrier Vehicle & Mobile Gun System
  - 11 different configurations/uses
- Lighter & more mobile than Abrams & Bradley
- Developed as interim for Future Combat Systems (FCS) Vehicles
- Goal is to deploy a Stryker Brigade worldwide in 96 hours

Stryker Brigade Combat Teams

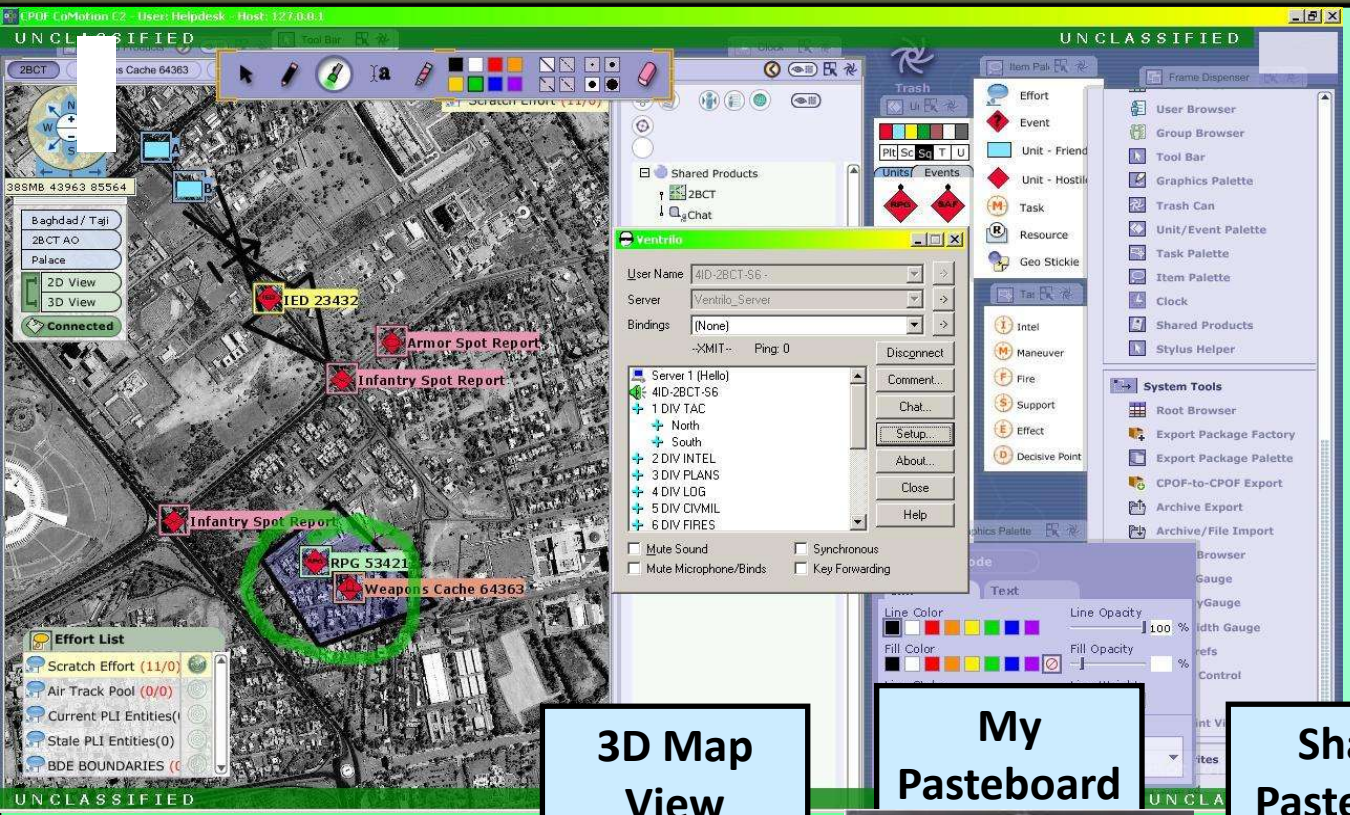
2/25 ID (SBCT)	1/25 ID (SBCT)	3/2 ID (SBCT)	4/2 ID (SBCT)	5/2 ID (SBCT)	56/28 ID (SBCT) PAANG	2CR (SBCT)
Schofield Barracks, Hawaii	Fort Wainwright Alaska	Fort Lewis, Washington	Fort Lewis, Washington	Fort Lewis, Washington	Pennsylvania	Germany



SBCT Warfighters' Forum (WfF)



Command Post of the Future (CPoF)



- ***Enables Near-Real Time Collaboration***
  - Dispersed Situational Awareness Tool
  - Common Operational Picture (COP)
  - Collaborate with live map, VoIP & "white board" highlighting
  - Visibility down to Company-level
  - Situational Awareness & 2-D to Disadvantage Users

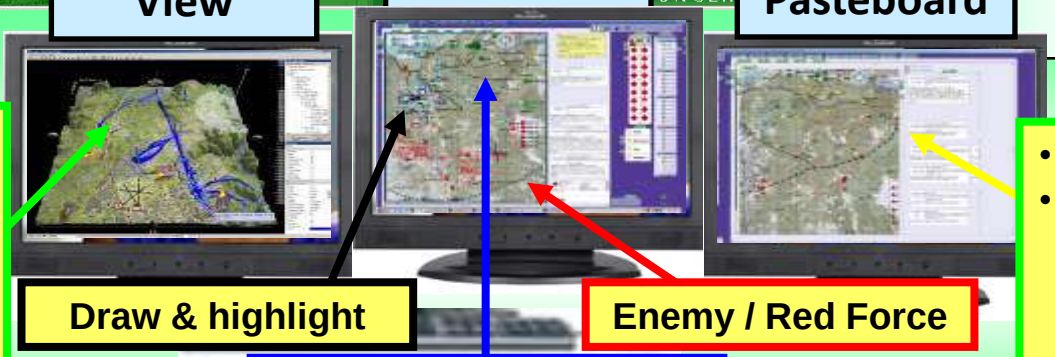
3D Map View

My Pasteboard

Shared Pasteboard

CPoF 3-screen Config

- **Provides 3-D picture**
- **Provide rapid terrain appreciation**
- **Linked to 2-D Map**
- **Allows 3-D Map manipulation**



Draw & highlight

Enemy / Red Force

Friendly / Blue Force

- **Real time updating**
- **Other Pasteboards**
  - **Master Schedule**
  - **SITREPs**
  - **All are Shareable**

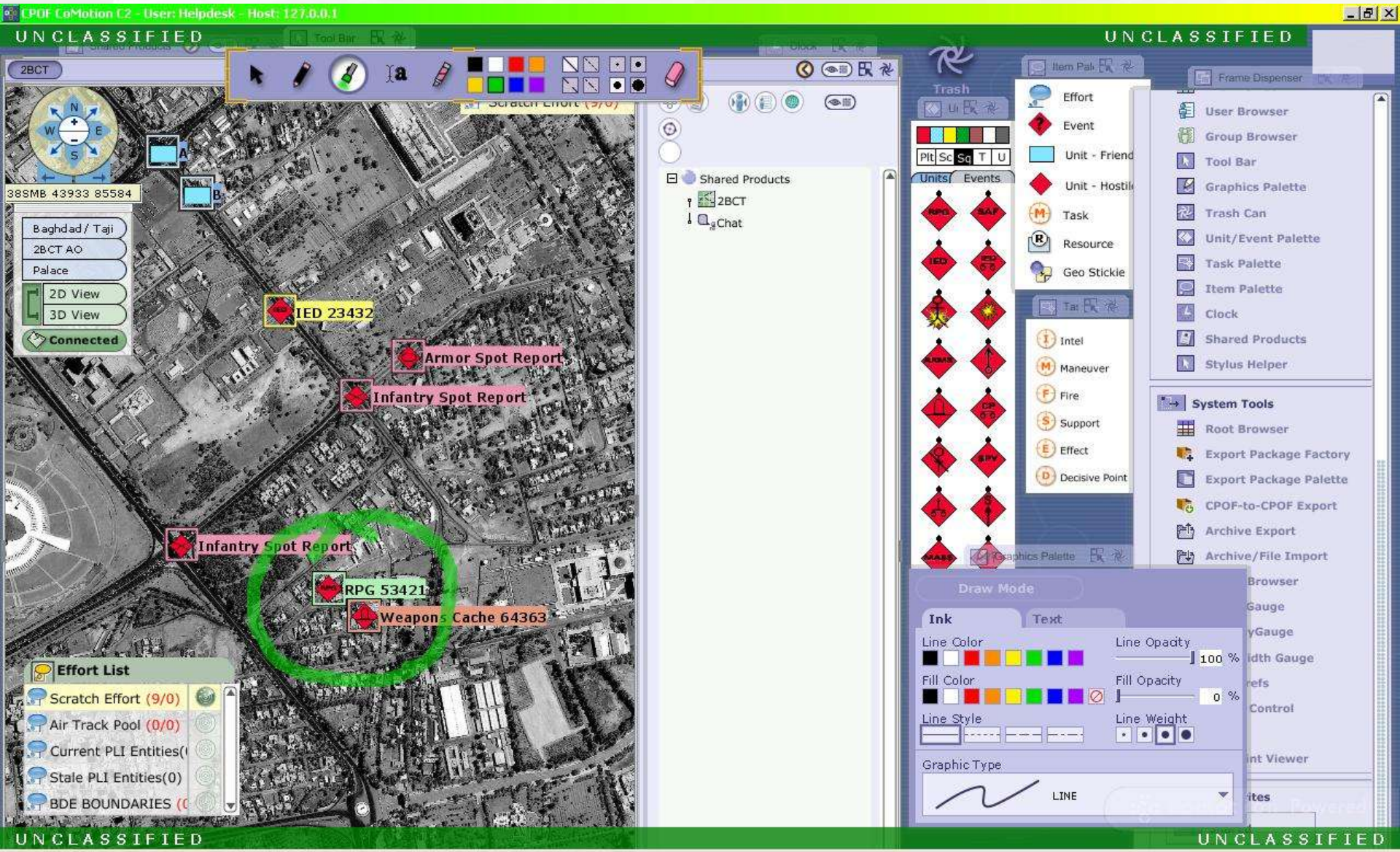
Command Post of the Future (CPoF)

Video "Whiteboard" & VoIP Collaboration

Command Post of the Future (CPoF)

Use of the Highlight Pen – Everyone watching this map will see the Green Circle as point-of-interest/discussion

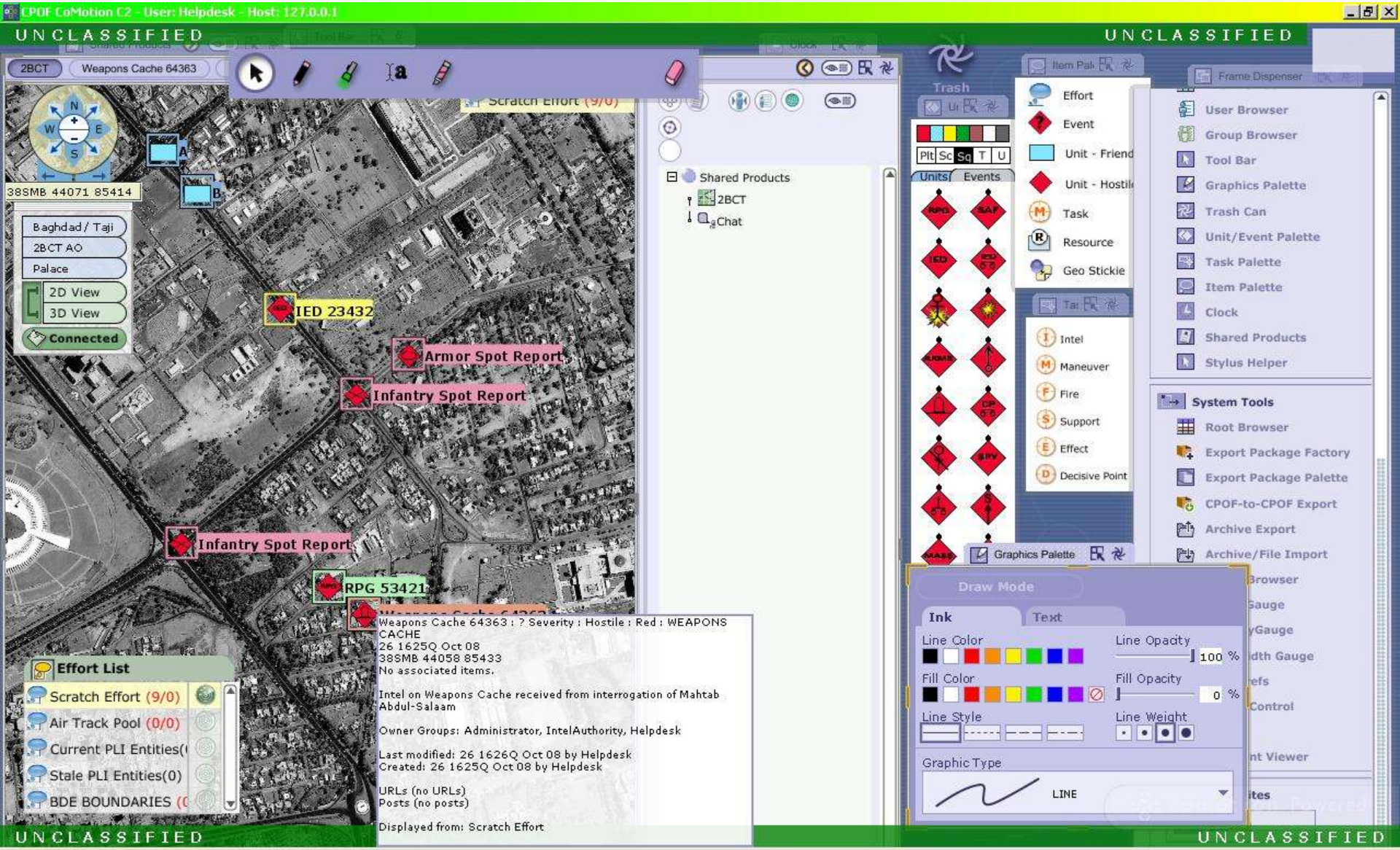
Command Post of the Future (CPoF)



Command Post of the Future (CPoF)

Tooltip Capabilities – Anyone watching this map can "pull up" the live data on the point-of-interest

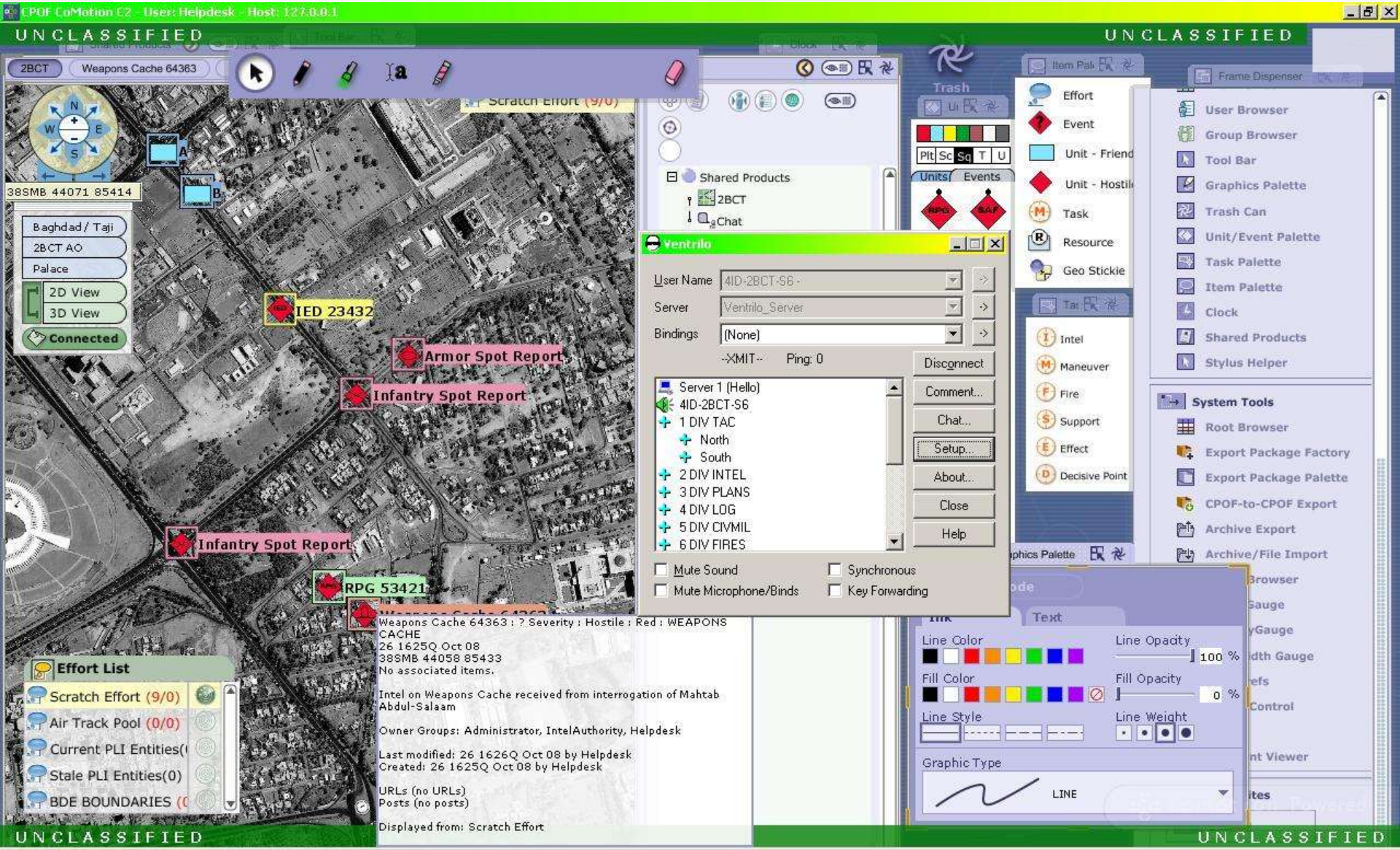
Command Post of the Future (CPoF)



Command Post of the Future (CPoF)

Ventrilo VoIP Client – allows online conversations between CPoF Users

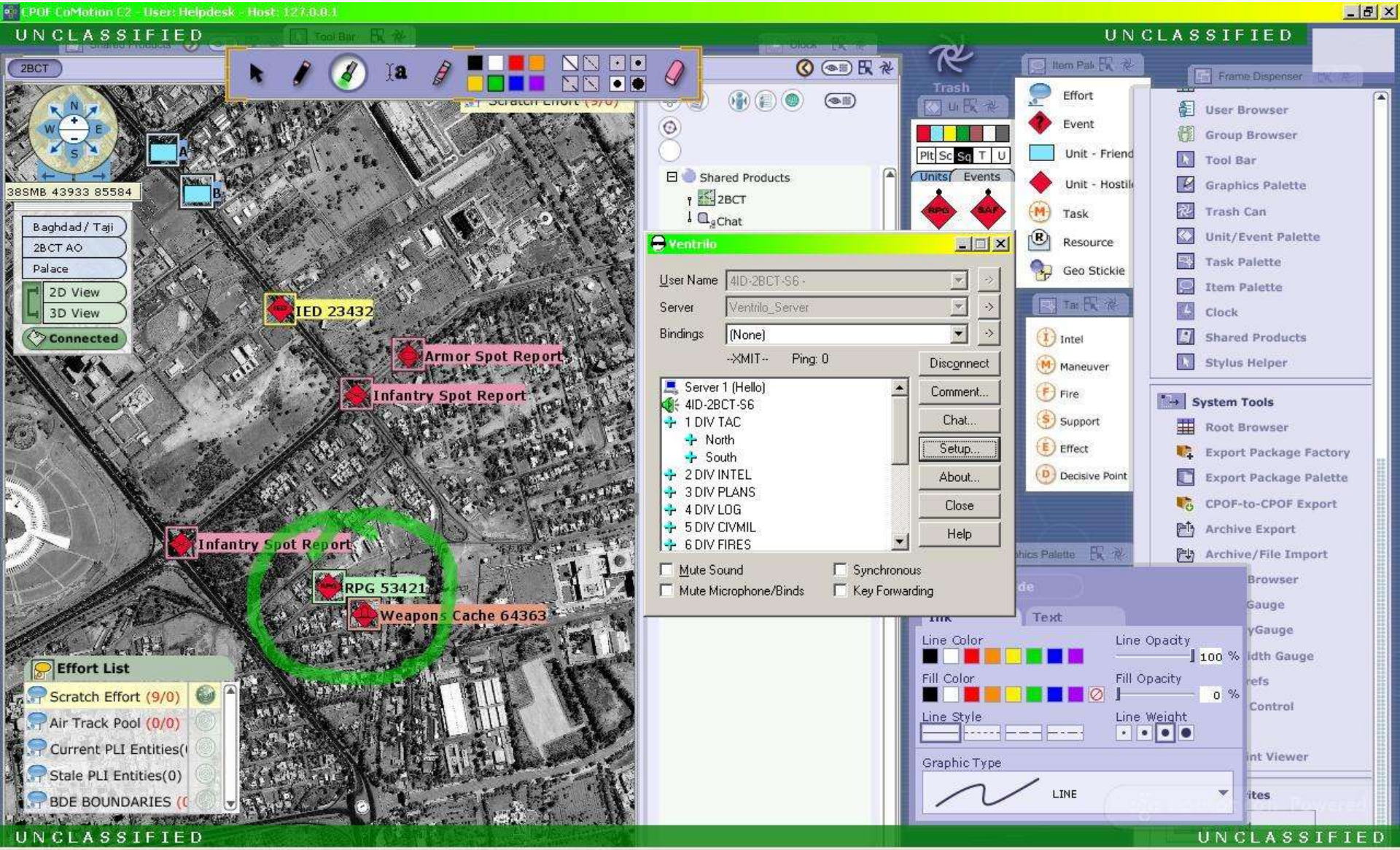
Command Post of the Future (CPoF)



Command Post of the Future (CPoF)

Use of the Highlight Pen & Ventrilo VoIP capabilities in conjunction to provide real-time collaboration

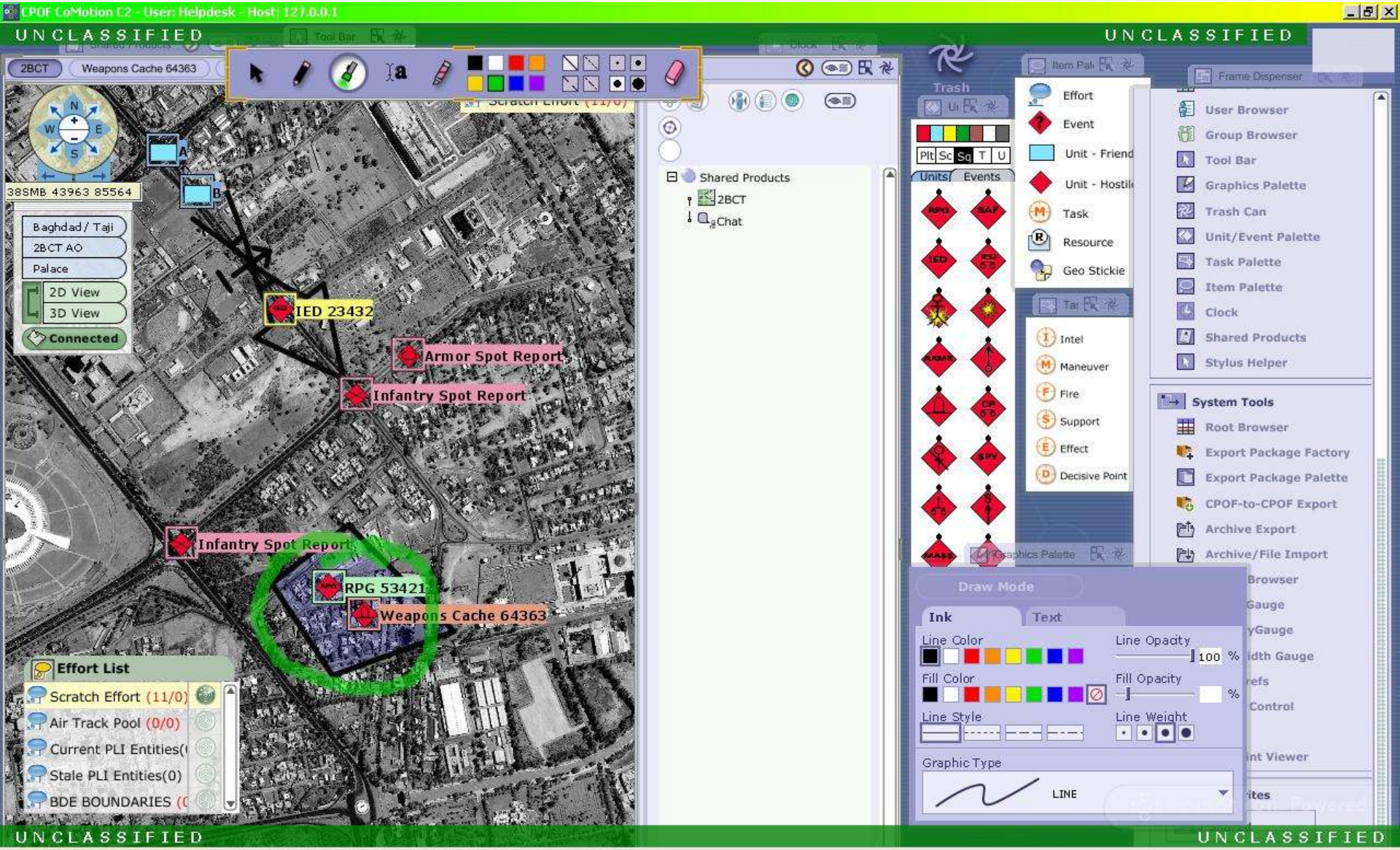
Command Post of the Future (CPoF)



Command Post of the Future (CPoF)

Use of tactical graphics (black arrow & black-outlined purple box) to direct actions of responding Elements

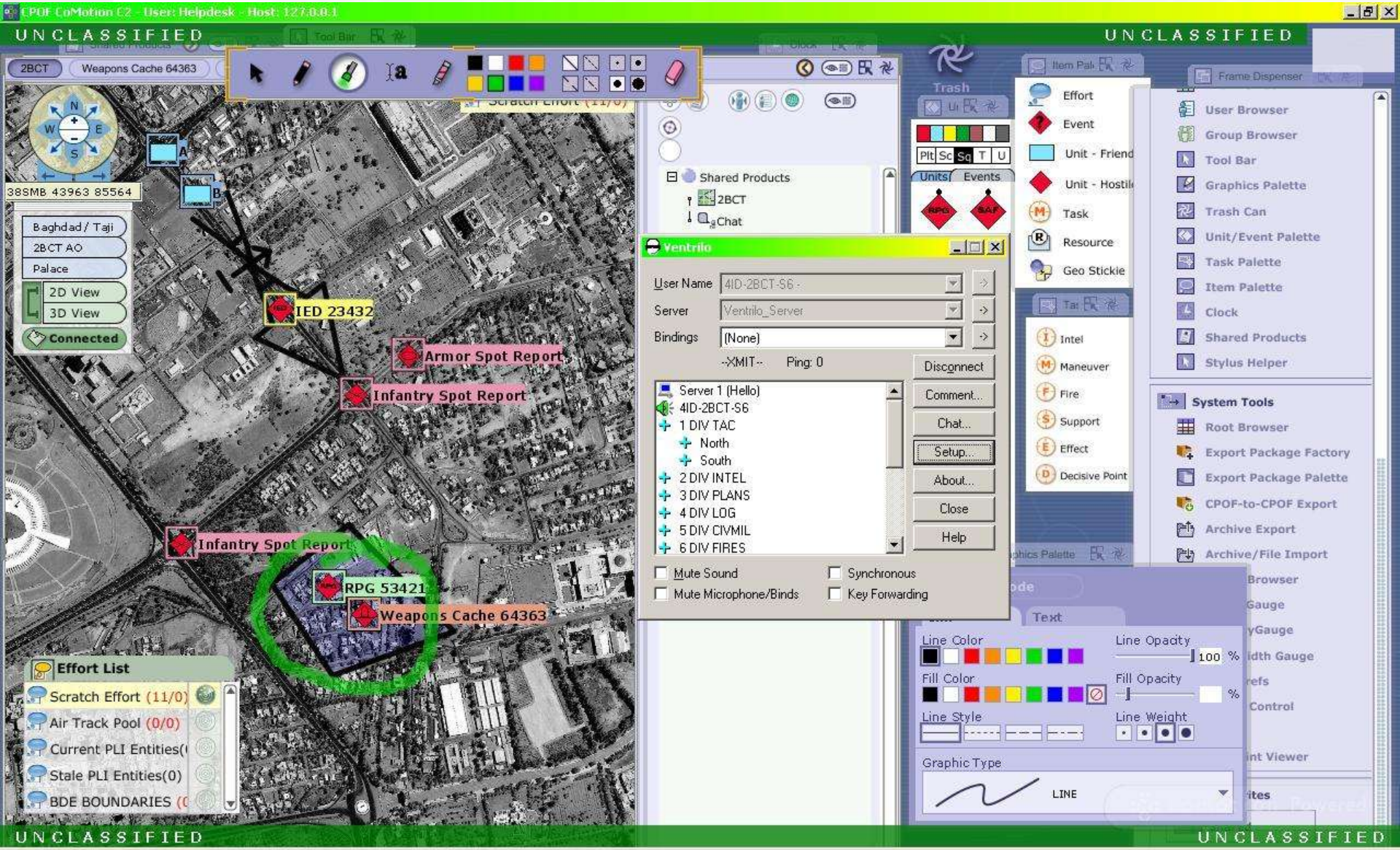
Command Post of the Future (CPoF)



Command Post of the Future (CPoF)

Use of Tactical Graphics & Ventrilo VoIP capabilities in conjunction to provide real-time collaboration

Command Post of the Future (CPoF)



Battle Command – Web 2.0

Google Earth

BC Platform Services Environment

Imagery

Map Collaboration (Chat)

Fires Maneuver LOG ...

Data Mediation

Security

Federated Chat

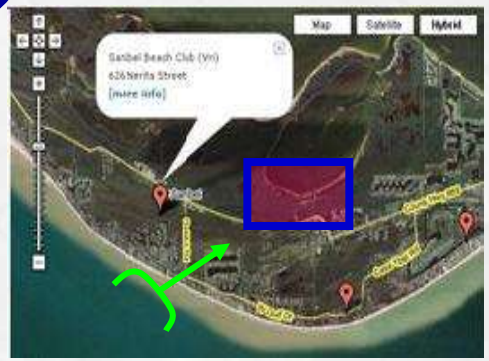
Maneuver

KML / Industry Standards

Mashup Methodology

BC Data / Collaboration Standards

Air



Warfighter View

CPoF

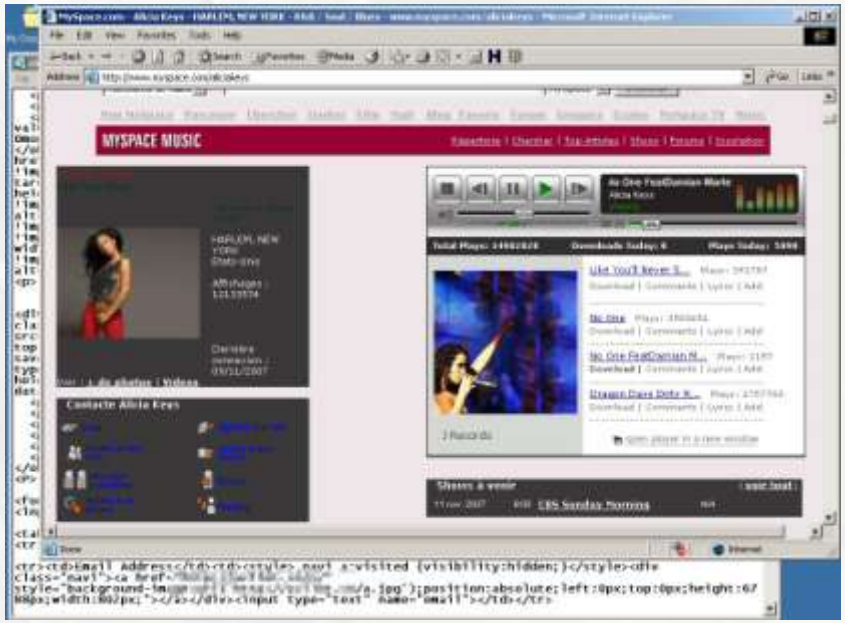
NGO / Industry

RSS Notifications

Battle Cmd Systems

Malware Threat

- Example: Facebook message sent with YouTube Link
- Link contains iFrame or user clicks to install update & installs malware on PC



- 28,940 different malicious & unwanted programs were detected on User PCs in Aug, a increase of 8,000 from Jul
- Projections are for a 10-fold increase in malware objects in 2008 – a 'hockey-stick' growth of ID theft & Cyber crime

Botnets

- In 2008 Botnets continued to become worse – a trend expected to continued next year
  - 2007 estimates 10% of online computers were in Botnets
  - 2008 estimates Botnets may comprise up to 15% of computers
- Botnets growing at faster rate than viruses or spam due to:
  - Infections can occur thru legitimate Web sites
  - Bot exploits/malware delivery are more sophisticated & obscure
  - Users need do nothing to become infected, e.g. visit a Website
- Botnets/Bot-Armies harness considerable computing power to engage in a variety of insidious & malicious activities
  - Data Theft (SSAN, Credit Cards, Trade Secrets, etc.)
  - DDoS Attacks
  - Spam Delivery
  - DNS Server Spoofing

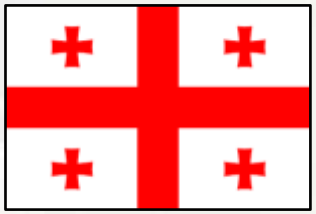
Cyber Warfare

GEORGIA

Source: Georgia Tech Information Security Center (GTISC) Report – October 15, 2008

Cyber Warfare

GEORGIA

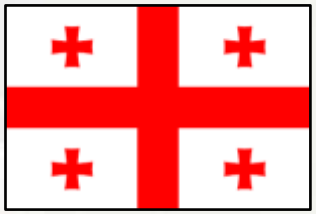


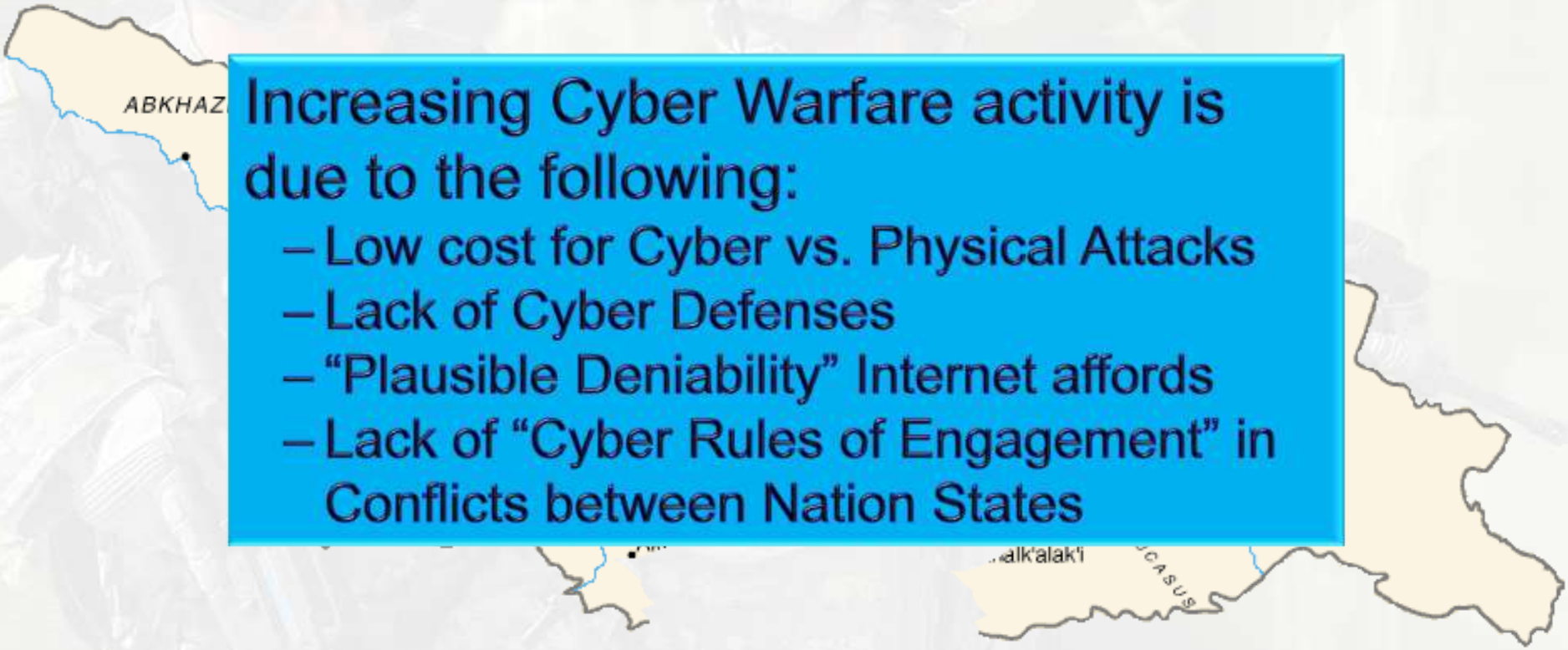
- In Future Warfare Cyber Warfare will accompany traditional military actions
- Consider recent attacks in Georgia:
  - Source of Russian Cyber Attacks included Internet Traffic thru Turkey & Azerbaijan
  - DDoS attacks crippled Georgia limited Internet, Media outlets & Government sites
  - Multiple means included Route Hijacking, Server Compromise, Data Theft & Fake Sites

Source: Georgia Tech Information Security Center (GTISC) Report – October 15, 2008

Cyber Warfare

GEORGIA





Increasing Cyber Warfare activity is due to the following:

- Low cost for Cyber vs. Physical Attacks
- Lack of Cyber Defenses
- "Plausible Deniability" Internet affords
- Lack of "Cyber Rules of Engagement" in Conflicts between Nation States

Source: Georgia Tech Information Security Center (GTISC) Report – October 15, 2008

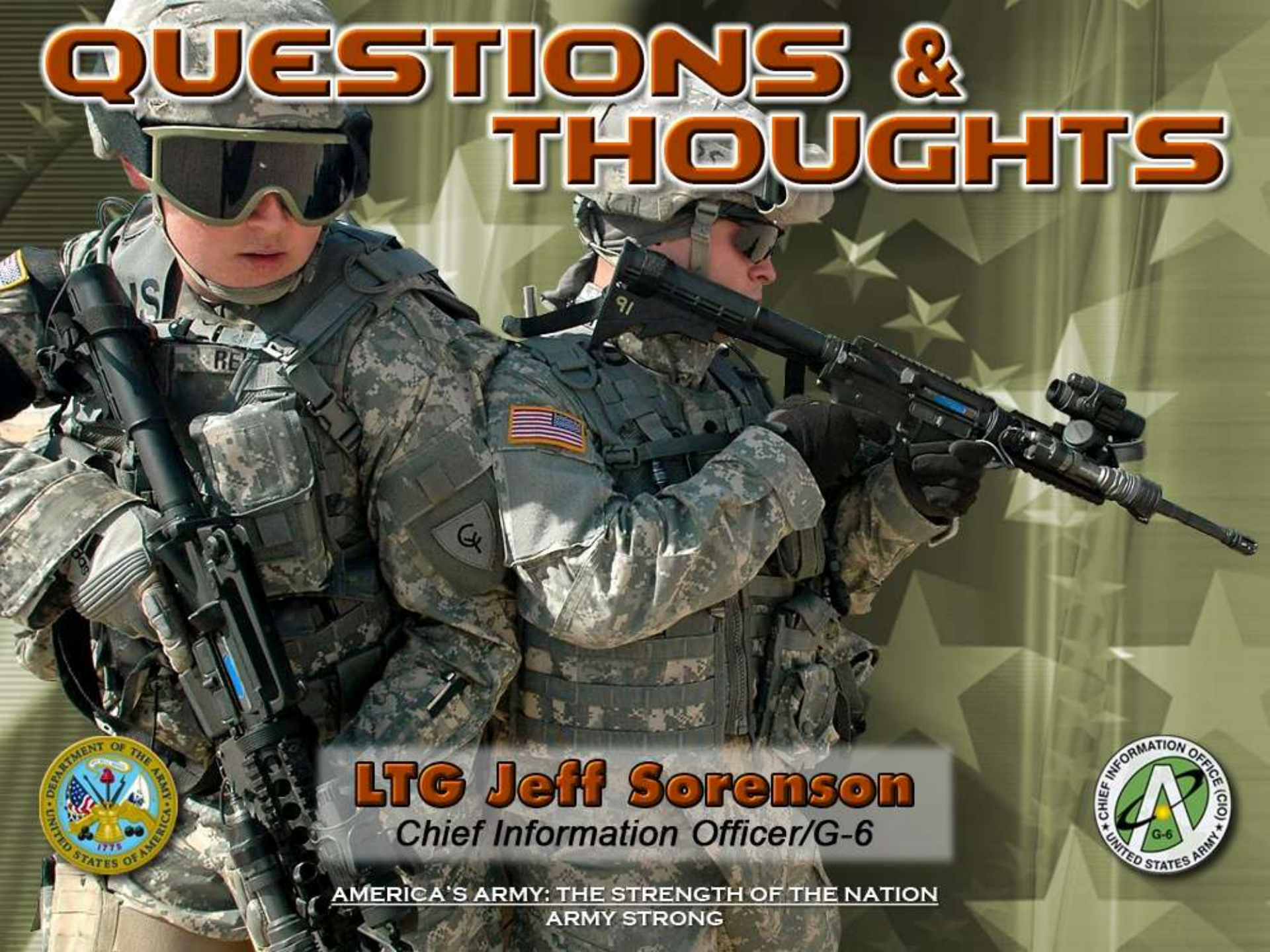
Conclusions!!!

- **Posturing for Persistent Conflict**
  …driving an Expeditionary Army

- **DoD Information Technology**
  …continuously lagging generation(s)
- **Army Way Ahead**
  …work comprehensive Web 2.0 effort with DoD & Industry
- **Assured Situational Awareness**
  *…**Bottom Line** to Joint Warfighter*

Army Strong!

QUESTIONS & THOUGHTS



LTG Jeff Sorenson

Chief Information Officer/G-6

AMERICA'S ARMY: THE STRENGTH OF THE NATION

ARMY STRONG

Service-Disabled Vet-Owned Small Business (SDVOSB) Opportunities

- Veterans Benefits Act of 2003 & Executive Order 13360 sets goal of 3% for SDVOSB Contracts
- Over 12,000 SDVOSB firms registered in Central Contractor Registration (CCR) Database
- Center for Veterans Enterprise maintain VetBiz Vendor Info Pages (VIP) Database
- Army Small Business Website useful resource for SDVOSB http://www.sellingtoarmy.info
- Government Services Agencies Website useful resource as well http://www.gsa.gov/portal